Tentamen i Krypteringsmetoder och Säkring av Datasystem

7.5 hp

2 juni, 2014 kl. 9.00 – 13.00

Maxpoäng: 30p. **Betygsgränser**: 12p: betyg G, 21p: betyg VG.
Hjälpmedel: Miniräknare samt formelsamling som medföljer tentamenstexten.
Kursansvarig: Eric Järpe, telefon 0702-822 844, 035-16 76 53.

Till uppgifterna skall *fullständiga lösningar* lämnas. Lösningarna ska vara *utförligt* redovisade! Varje lösning ska börja överst på nytt papper. Endast en lösning per blad. Lösningar kommer finnas på internet: `http://dixon.hh.se/erja/teach` → `Krypteringsmetoder och säkring av datasystem.`

1. Beskriv proceduren vid *signering* med RSA systemet. (3p)

2. Beräkna gcd till
   (a) 14 040 och 59 895. (3p)
   (b) $12\,012x$, $10\,140y$ och $13\,260z$ där x, y och z är relativt prima. (4p)

3. Vad hette de två personer som knäckte problemet med nyckelutbyte genom att uppfinna en algoritm för asymetriska krypton? (Efternamnen räcker.) (2p)

4. Förklara kortfattat vad som menas med *Bibelkoden*. (3p)

5. Vad innebär steganografi? (2p)

6. Beräkna den principala resten av $13^{57} + 24^{68}$ vid heltalsdivision med 9. (3p)

7. Vad innebär födelsedagsparadoxen? (3p)

8. Nämn 3 hashfunktioner som använts i stor skala. (3p)

9. Man vill konstruera minst 1 miljard lösenord som ska vara minst 7 tecken långa. Hur många tecken måste man ha i det alfabet man använder då lösenorden konstrueras? (4p)

LYCKA TILL!